

KELLEY DRYE & WARREN LLP

A LIMITED LIABILITY PARTNERSHIP

WASHINGTON HARBOUR, SUITE 400

3050 K STREET, NW

WASHINGTON, D.C. 20007-5108

(202) 342-8400

NEW YORK, NY

CHICAGO, IL

STAMFORD, CT

PARSIPPANY, NJ

BRUSSELS, BELGIUM

AFFILIATE OFFICES

MUMBAI, INDIA

FACSIMILE

(202) 342-8451

www.kelleydrye.com

DIRECT LINE: (202) 342-8640

EMAIL: ckoves@kelleydrye.com

February 28, 2011

VIA ECFS

Marlene H. Dortch
Office of the Secretary
Federal Communications Commission
445 12th Street S.W.
Washington, D.C. 20554

**RE: 2011 Annual Customer Proprietary Network Information Compliance
Certification; EB Docket No. 06-36**

Dear Secretary Dortch:

Please find attached the 2011 Annual Customer Proprietary Network Information
("CPNI") Compliance Certification for Bresnan Communications, LLC.

Please contact the undersigned if you have any questions regarding this filing.

Respectfully Submitted,



Christopher S. Koves
Counsel to Bresnan Communications, LLC

Attachment

BRESNAN COMMUNICATIONS, LLC

ANNUAL 47 C.F.R. § 64.2009(e) CPNI CERTIFICATION

EB DOCKET 06-36

Annual Section 64.2009(e) CPNI Certification for calendar year 2010.

Name of Companies: Bresnan Communications, LLC
 Bresnan Broadband of Montana, LLC
 Bresnan Broadband of Wyoming, LLC
 Bresnan Broadband of Colorado, LLC
 Bresnan Broadband of Utah, LLC

Form 499 Filer ID: 824408 (Bresnan Communications, LLC)

Name of Signatory: James Nuzzo

Title of Signatory: Executive Vice President, Business Planning

I, James Nuzzo, certify that I am an officer of the company named above ("Company"), and acting as an agent of the Company, that I have personal knowledge that the Company has established operating procedures that are adequate to ensure compliance with the Federal Communications Commission's ("Commission's" or "FCC's") Customer Proprietary Network Information ("CPNI") rules. *See 47 C.F.R. § 64.2001 et seq.*

Attached to this certification is an accompanying statement explaining how the Company's procedures ensure that the Company is in compliance with the requirements set forth in section 64.2001 *et seq.* of the Commission's rules. *See 47 C.F.R. § 64.2009(e).*

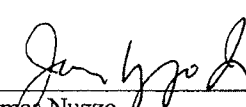
The Company has not taken any actions (*i.e.* proceedings instituted or petitions filed at either state commissions, the court system, or at the Commission) against data brokers during the above-referenced certification period. The Company also has no knowledge or experience regarding the specific processes pretexters are using to attempt to access CPNI. The steps that the Company is taking to protect CPNI are described in the attached statement that summarizes the Company's operating procedures for compliance with the Commission's CPNI rules. The Company has not received any customer complaints concerning the unauthorized release of CPNI during the above-referenced certification period.

This certification is made to the best of my knowledge, information and belief.

Dated: _____

2/28/11

Signed: _____


James Nuzzo
Executive Vice President, Business Planning
Bresnan Communications, LLC
Bresnan Broadband of Montana, LLC
Bresnan Broadband of Wyoming, LLC
Bresnan Broadband of Colorado, LLC
Bresnan Broadband of Utah, LLC

**STATEMENT REGARDING OPERATING PROCEDURES
IMPLEMENTING 47 C.F.R. SUBPART U
GOVERNING USE OF
CUSTOMER PROPRIETARY NETWORK INFORMATION (CPNI)**

Bresnan Communications, LLC, Bresnan Broadband of Montana, LLC, Bresnan Broadband of Wyoming, LLC, Bresnan Broadband of Colorado, LLC, and Bresnan Broadband of Utah, LLC (collectively, "Bresnan" or "the Company") are committed to protecting the privacy of its customers' confidential and proprietary information and have established operating procedures to protect Customer Proprietary Network Information ("CPNI"). The following statement explains the operating procedures of the Company to ensure that it is in compliance with the CPNI rules of the Federal Communications Commission ("Commission" or "FCC").

Bresnan trains employees on the limitations of use or disclosure of CPNI as governed by federal law and Bresnan policy. Bresnan's policy, administered by its CPNI Compliance Officer, establishes the procedures and safeguards regarding Bresnan's use and disclosure of CPNI set forth below.

I. USE, DISCLOSURE OF, AND ACCESS TO CPNI

Bresnan will use, disclose, or permit access to CPNI only in its provision of the communications service from which such information is derived. The Company also uses CPNI for various purposes permitted by law. For example, the Company may use, disclose or permit access to CPNI:

- a. for services necessary to, or used in, the provision of such communications service, including the publishing of directories;
- b. to initiate, render, bill and collect for communications services;
- c. to protect the rights or property of Bresnan, or to protect users or other carriers or service providers from fraudulent, abusive or unlawful use of, or subscription to, such services;
- d. to provide inside wiring installation, maintenance, or repair services;
- e. as required by law; or
- f. as expressly authorized by the customer.

Bresnan does not use CPNI to market services. Bresnan has established a supervisory review process regarding its compliance with the FCC's CPNI rules for marketing situations and maintains records of carrier compliance for a minimum period of one year. In the event that any employee or agent wishes to use CPNI for marketing, such proposed use is subject to a supervisory review process that shall involve a supervisor designated by the senior employee responsible for marketing or the CPNI Compliance Officer. If such use is approved, Bresnan shall modify these policies and conduct additional training as needed to assure compliance with the FCC's rules.

Bresnan does not use, disclose or permit access to CPNI to identify or track customers that call competing service providers. When Bresnan receives or obtains proprietary information from another carrier for purposes of providing a telecommunications service, it shall use such information only for such purpose, and shall not use such information for its own marketing efforts.

II. PROTECTION OF CPNI

Above and beyond the specific FCC requirements, Bresnan will take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI. If any employee becomes aware of new methods that are being used or could be used by third parties to attempt to obtain

unauthorized access to CPNI, or of possible changes to Bresnan's existing policies that would strengthen protection of CPNI, they should report such information immediately to Bresnan's CPNI Compliance Officer so that Bresnan may evaluate whether existing policies should be supplemented or changed.

A. Inbound Calls to Bresnan Requesting CPNI

Bresnan's customer service representatives (CSRs) may not disclose any CPNI to an inbound caller until the caller's identity has been authenticated. For CPNI not including Call Detail Information (CDI), CSRs authenticate callers by requesting their telephone number, account number, name and address.

Bresnan CSRs do not reveal any Call Detail Information (CDI) to inbound callers. The CSRs that answer inbound telephone calls do not have access to CDI. CDI includes any information that pertains to the transmission of specific telephone calls, including: (1) for outbound calls, the number called, and the time, location, or duration of any call; and (2) for inbound calls, the number from which the call was placed, and the time, location, or duration of any call. Bresnan's ordinary policy is to provide the requested CDI by sending the information by mail to a mailing address of record for the account but only if such address has been on file with Bresnan for at least 30 days.

B. Online Accounts

Bresnan customers may obtain certain telephone account information from certain online sources accessed from the Bresnan website. To access these on-line accounts, the customer must enter a login ID that they create and a password established in accordance with the criteria established by Bresnan. Bresnan has in place detailed procedures in the event a customer needs to create a new login ID/password, forgets their login ID/password and needs to reset, or needs to change their login ID/password.

C. In-Person Disclosure of CPNI at Bresnan Offices

Bresnan may disclose CPNI to a customer visiting a Bresnan office if they present a valid photo ID matching the customer's account information. A valid photo ID is a government-issued means of personal identification with a photograph such as a driver's license, passport, or comparable ID that is not expired.

D. Notice of Account Changes

When an online account is created or when a password or PIN is changed, Bresnan will mail a notification to customer's address of record notifying them of the change. When an address of record is created or changed, Bresnan will send a notice to a customer's preexisting address of record notifying them of the change. These notifications are not required when the customer initiates service. Each of the notices provided under this paragraph will not reveal the changed information and will direct the customer to notify Bresnan if they did not authorize the change.

E. Business Customer Exemption

Pursuant to 47 C.F.R. § 64.2010(g), the authentication requirements for disclosure of CPNI do not apply to disclosure of business customer information where the business customer has a dedicated account representative and a contract between Bresnan and that business customer that specifically addresses the protection of CPNI.

F. Audit Trail

All instances of each employee access to a customer account are logged and the logs are maintained for a reasonable time. Bresnan accordingly has access to an audit trail of all such access that shall be consulted in the event that a breach of a customer's CPNI is detected.

G. Data Retention

Bresnan destroys customer information that is no longer necessary for the purpose for which it is collected unless there is a legitimate request or order to inspect the information still outstanding or the information remains in routine records that are periodically discarded under the Company's document retention policies.

III. REPORTING CPNI BREACHES TO LAW ENFORCEMENT

Any Bresnan employee that becomes aware of any breaches, suspected breaches or attempted breaches must report such information immediately to the Bresnan CPNI Compliance Officer. Such information must not be reported or disclosed by any employee to any non-employee, including the potentially affected customer, except in express conformance with the procedures described below. Any employee that fails to report such information will be subject to disciplinary action that may include termination.

It is Bresnan's policy that employees should not be discouraged from reporting information about breaches that may have been caused in part by their own actions or omissions. Once a breach has occurred, the most important objective is to attempt to limit the damage to customers, to make any adjustments as needed to prevent a recurrence of the breach, and to alert law enforcement promptly. Therefore, although employees who violate Bresnan's CPNI policies are subject to discipline, the sanctions may be substantially reduced where employees promptly self-report violations if appropriate.

A. Identifying a Breach

A breach has occurred when a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI. If an employee has information about an incident and is not certain that the incident would not constitute a breach under this definition, the incident must be reported to the CPNI Compliance Officer. If a Bresnan employee determines that an unauthorized person is attempting to gain access to CPNI but does not succeed at doing so, no breach has occurred. However, the incident must be reported to Bresnan's CPNI Compliance Officer who will determine whether to report the incident to law enforcement and/or take other appropriate action. Bresnan's CPNI Compliance Officer will also determine whether it is appropriate to update Bresnan's CPNI policies or training materials in light of any new information.

B. Notification Procedures

As soon as practicable, and in no event later than 7 business days upon learning of a breach, the Bresnan CPNI Compliance Officer shall electronically notify the U.S. Secret Service ("USSS") and the Federal Bureau of Investigation ("FBI") of the breach via the central reporting facility www.cpnireporting.gov. If this link is not responsive, Bresnan's policy is to contact counsel or the FCC's Enforcement Bureau (<http://www.fcc.gov/eb/cpni>) for instructions. Bresnan will not notify customers or disclose a breach to the public until 7 full business days have passed after notification to the USSS and the FBI, except as provided below. If Bresnan receives no response from either the USSS or FBI after the

7th full business day, it must promptly proceed to inform the customers whose CPNI was disclosed of the breach.

Bresnan will delay notification to customers or the public upon request of the FBI or USSS. If the Bresnan CPNI Compliance Officer believes there is a need to disclose a breach sooner, he or she should so indicate in the notification to law enforcement. However, such notification does not itself permit notice to customers; Bresnan still may not notify customers sooner unless given clearance to do so from *both* the USSS and the FBI.

IV. RECORD RETENTION

The Bresnan CPNI Compliance Officer is responsible for assuring that Bresnan maintains for at least two years a record, electronically or in some other manner, of any breaches discovered, notifications made to the USSS and the FBI pursuant to these procedures, and notifications of breaches made to customers. The record must include, if available, dates of discovery and notification, a detailed description of the CPNI that was the subject of the breach, and the circumstances of the breach.

Bresnan maintains a record, for a period of at least one year, of those limited circumstances in which CPNI is disclosed or provided to third parties or where third parties were allowed access to CPNI. Because Bresnan does not use CPNI for marketing or for any other purpose for which customer approval is required, it does not have any records to keep regarding supervisory review of marketing; or of sales and marketing campaigns that use CPNI; or of records associated with customers opt-out approval or non-approval to use CPNI, or notification to customers prior to any solicitation for customer approval to use or disclose CPNI.

Bresnan will maintain a record for at least two years of any customer complaints related to its handling of CPNI, and records of Bresnan's handling of such complaints. The CPNI Compliance Officer will assure that all complaints are reviewed and that Bresnan considers any necessary changes to its policies or practices to address the concerns raised by such complaints.

V. TRAINING

All employees with access databases that include CPNI receive a copy of Bresnan's CPNI policies and are informed that: (1) any use or disclosure of CPNI or other act or omission not in compliance with such policies will result in disciplinary action, including the termination of employment where appropriate; and (2) employees who knowingly facilitate the unauthorized disclosure of a customer's confidential information may be subject to criminal penalties. In addition, Bresnan conducts mandatory CPNI training for all CSRs, personnel at retail offices that may receive requests for CPNI, technical support personnel who field calls from customers, provisioning personnel who have access to and research customer inquiries regarding CDI, and marketing personnel.